IBM Comments

Third AES Conference
April 13, 2000

**Don Coppersmith, Rosario Gennaro, Shai Halevi, Charanjit Jutla,
Stephen M. Matyas Jr., Mohammad Peyravian, David Safford, Nevenko Zunic**

Introduction:

All five of the AES finalist candidates are solid ciphers, with no known weaknesses. It seems likely that any of the candidates would make a good standard. In this short paper, we summarize some qualitative and objective comments on the finalists, and make recommendations for final selection.

General Comments on the Candidates

MARS

MARS has one of the widest security margins, both in terms of number of rounds, and in terms of diversity (as its security relies on a combination of several different "strong operations" and on a heterogeneous structure). MARS is the only candidate with a heterogeneous structure, which was a deliberate design feature to help resist unknown attacks. Also, the design of the round function in MARS lends itself to analysis. In particular, a nearly complete characterization is known for the differential behavior of the round function, and independent analysis has been published.

At the same time, MARS is also a very fast cipher. In fact, in some of the measurements, MARS posted the fastest C and Java benchmarks. In Gladman's C benchmarks, MARS average performance across all key sizes was second only to RC6.

One concern raised about MARS was that it was hard to implement on memory constrained environments. In response to this criticism, the key schedule was tweaked prior to round 2, significantly reducing memory requirements.

Another criticism raised about MARS concerned its complexity. We feel that this was partly due to our extremely detailed presentation and analysis of the algorithm. We subsequently released a simplified description including simplified pseudocode which fits on a single page, (which is included later in this paper). In addition, using implementation lines as a complexity measurement, MARS is ***less*** complex than Twofish, Rijndael, and Serpent.

RC6

RC6 has a simple, elegant round function, and it is the fastest cipher in speed tests. A possible concern about RC6 is that its round function may be "too simple". Specifically, the combination of multiplications and rotation, although providing some excellent properties, is

a "single point of failure" in RC6 (as it does not use S−boxes). Also, RC6 seems to have the lowest security margin of the candidates in terms of number of rounds.

Rijndael

Rijndael is a fast cipher, which is very flexible for implementation. It is important to note that its speed on 256 bit keys is lower than MARS or Twofish.

Rijndael has a round function which is hard to analyze, and a key schedule that makes it easier to mount power attacks. Also, the fact that the round function can be expressed as only a few simple algebraic operations makes one wary of potential algebraic attacks against it.

The structure of Rijndael and Square is new, and not fully understood. In "The Block Cipher Square", Daemen, Knudsen, and Rijmen presented an attack unique to the Square structure, which caused them to increase the number of rounds. The existence of attacks unique to Square call into question Rijndael's long term resistance.

Rijndael's mode with only 10 rounds has a relatively low security margin.

Serpent

Serpent has very wide security margins in terms of number of rounds, and very strong mixing. On the down side, it is quite slow, and it also has a key schedule that makes power attacks easier to mount. As there are other candidates with good security margins, and much faster performance, we feel that Serpent is too slow.

Twofish

Twofish is a flexible cipher in terms of implementation tradeoffs, and it is also one of the fastest ciphers (except for its key−schedule). It has good security margins, and reasonable complexity.

A concern about Twofish is that it is very hard to analyze its security. Its round function was engineered to provide flexibility, rather than to facilitate analysis. Indeed, although a lot of effort has already been invested in its analysis, it is safe to say that the exact properties of the round function are not very well understood. Moreover, the reliance on key dependent S−boxes which are not generated pseudorandomly, makes the analysis even harder.

Another drawback of the key dependent S−boxes is that they are inherently more costly. In Twofish this extra cost can be shifted between the key−setup and the cipher, but nonetheless it is always there. Finally, the key schedule of Twofish makes power attacks easier, since the entire key can be deduced from only the initial whitening key.

Complexity/Size of the Candidates

As mentioned earlier, MARS is actually not a complex algorithm. One way to measure complexity is to count lines needed to implement the cipher. Here are some measurements of Gladman's C code implementations, which can be used to compare complexity:

Cipher	Lines	LOC	Statements
RC6	116	71	86
MARS	424	298	249
Twofish	496	346	224
Rijndael	449	282	212
Serpent	623	479	620

(*Lines* counts the lines in the implementation, including comments and blanks; *LOC* (lines of code) counts only lines with statements, and *statements* counts the number of C statements.) As expected, RC6 is significantly simpler. Surprisingly, Serpent is significantly more complex to implement. MARS, Twofish, and Rijndael fall in the middle, with comparable complexity. In addition, to show the conceptual simplicity of MARS, here is the entire pseudocode for MARS encryption in 30 lines, (counting comments and blank lines).

```
// Forward Mixing
(A,B,C,D) = (A,B,C,D) + (K0,K1,K2,K3)
For i = 0 to 7 {
  B = (B ^ S0[A]) + S1[A>>>8]
  C = C + S0[A>>>16]
  D = D ^ S1[A>>>24]
  A = (A>>>24) + B(if i=1,5) + D(if i=0,4)
 (A,B,C,D) = (B,C,D,A)
}

// Keyed Transformation and E−Function
For i = 0 to 15 {
  R = ((A<<<13) * K[2i+5]) <<< 10
  M = (A + K[2i+4]) <<< (low 5 bits of (R>>>5))
  L = (S[M] ^ (R>>>5) ^ R) <<< (low 5 bits of R)
  B = B + L(if i<8) ^ R(if i>=8)
  C = C + M
  D = D ^R(if i<8) + L(if i>=8)
 (A,B,C,D) = (B,C,D,A<<<13)
}

// Backward Mixing
For i = 0 to 7 {
  A = A − B(if i=3,7) − D(if i=2,6)
  B = B ^ S1[A]
  C = C − S0[A<<<8]
  D = (D − S1[A<<<16]) ^ S0[A<<<24]
 (A,B,C,D) = (B,C,D,A<<<24)
}
(A,B,C,D) = (A,B,C,D) − (K36,K37,K38,K39)
```

Performance, Complexity, and Relative Security Margin

In this section we have collected and summarized some measurements of performance, and complexity, and estimates of security margin. For performance, we use Gladman's C code results [1]. Note that Rijndael's performance varies based on key size. While other papers have analyzed the candidates on other platforms, only performance on the NIST selected reference platform has received adequate analysis and review, so we use those numbers here.

As a simple complexity measurement, we count lines in Gladman's C implementations [2]. As these have all been written by the same person to the same API, with the same style, the line counts indicate relative complexity. For security margin, we use Biham's analysis [3] of rounds divided by minimum secure rounds, to get a ratio, in which large numbers represent higher (better) margins.

Cipher	Speed(Mb/sec)	Setup(Clocks)	Lines	Security Margin
RC6	94.2	1875	116	**1.0**
Mars	69.4	2134	424	1.6
Twofish	68.8	**8493−15616**	496	1.6
Rijndael	50.5−70.3	207−1983	449	1.3−1.8
Serpent	**26.7**	1296	**623**	1.9

In this table, we have **highlighted** values that are less competitive compared to the other candidates. This table makes clear the tradeoffs between speed and margins. RC6 is fastest, with the lowest margin. Serpent is slowest with the highest margin. The Serpent code is surprisingly more complex than the others, while RC6 is, as expected, the simplest code, with the others comparable between the extremes.

Recommendation Summary

RC6 is an elegant, fast, and well analyzed cipher, and would normally be considered the obvious best candidate, but for a standard that is supposed to last twenty years, its security margin is perhaps a bit too close to the edge. If only one candidate is chosen, RC6 is perhaps a bit risky.

Of the other ciphers, Serpent is too slow. Rijndael's structure is new and less well understood, and it has a slight disadvantage in performance with large keys. The security of Twofish is difficult to analyze, given its key dependent S−box, and it has a slight disadvantage in key setup performance. Since MARS has well understood and analyzed components, has a solid security margin, is fast, and does not have the large key or key setup performance problems, it is the best choice.

Should two candidates be selected, we feel that RC6 would be the obvious second choice, since the risk from its low margin would be much less of an issue, given the existence of the other cipher to fall back on. Its simplicity and tiny size make it very easy to add as a second cipher to any implementation.

References:

1. http://www.btinternet.com/~brian.gladman/cryptography_technology/aes2/ index.html
2. http://www.btinternet.com/~brian.gladman/cryptography_technology/aes2/aes.r2.algs.zip
3. http://www.cs.technion.ac.il/~biham/Reports/aes−comparing−revised.ps.gz